

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA)

Case No.

08 CR 10224 DPW

VIOLATIONS:

v.)

18 U.S.C. § 371 (Conspiracy)

18 U.S.C. § 1030(a)(2)(C) (Unauthorized Access to
Computer Systems)

18 U.S.C. § 1029(a)(3) (Access Device Fraud)

18 U.S.C. § 1028A (Aggravated Identity Theft)

CHRISTOPHER SCOTT,)

18 U.S.C. §§ 1029(c)(1)(C), 982(a)(2)(B), 981(a)

(1)(C), 28 U.S.C. § 2461(c) (Criminal Forfeiture)

Defendant.)

INFORMATION

COUNT ONE

(Conspiracy)

18 U.S.C. § 371

The U.S. Attorney charges that:

1. From approximately 2003 through 2008, in the Southern District of Florida, the District of Massachusetts and elsewhere,

CHRISTOPHER SCOTT,

and others known and unknown to the U.S. Attorney, did willfully conspire to commit the following offenses against the United States:

- a. Unlawful Access to Computers (18 U.S.C. § 1030(a)(2)(C)) – by means of interstate communications, intentionally accessing without authorization computers, which were used in interstate commerce, and thereby obtaining information from those computers, including credit and debit card information, for the purposes of commercial advantage and private

financial gain;

- b. Access Device Fraud (18 U.S.C. § 1029(a)(3)) – knowingly and with intent to defraud, possessing at least fifteen unauthorized access devices, to wit: stolen credit and debit card numbers;
- c. Wire Fraud (18 U.S.C. § 1343) – having devised and executed a scheme to defraud, and to obtain money and property by means of false and fraudulent pretenses, representations, and promises, transmitting and causing to be transmitted, in interstate commerce, wire communications, including writings, signals and sounds, for the purpose of executing the scheme to defraud;
- d. Aggravated Identity Theft (18 U.S.C. § 1028A) – knowingly transferring, possessing and using without lawful authority, a means of identification of other persons – to wit: credit and debit card account numbers of individuals – during and in relation to the commission of wire fraud (in violation of 18 U.S.C. §1343);
- e. Money Laundering (18 U.S.C. § 1956(a)(1)(B)(i) and (a)(2)(B)(i)) – knowing that the financial transactions, transmittals and transfers were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity and that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, (i) knowingly conducting and attempting to conduct financial transactions affecting

interstate and foreign commerce, which involved the proceeds of said specified unlawful activity, and (ii) knowingly transmitting and transferring funds from a place inside the United States to and through a place outside the United States and to a place inside the United States from and through a place outside of the United States.

Manner and Means of the Conspiracy

2. SCOTT and his co-conspirators, known and unknown to the U.S. Attorney, employed the following manner and means and others in furtherance of the conspiracy:
 - a. The conspirators unlawfully gained electronic access to corporate computer networks using various techniques;
 - b. The conspirators downloaded from those computer networks customers' credit and debit card information;
 - c. The conspirators fraudulently used the credit and debit card information to obtain cash advances and sold the information to others for fraudulent use by them; and
 - d. The conspirators moved money through Internet currency exchanges and bank accounts in Latvia to conceal and disguise the nature, location, source, ownership and control of the proceeds of this activity.

Overt Acts

3. In furtherance of the conspiracy and to effect its objects, SCOTT and his co-conspirators committed the following overt acts, among others:
 - a. In or about 2003, Gonzalez identified payment card data which was

accessible at an unencrypted wireless access point utilized by a BJ's Wholesale Club store. Gonzalez and SCOTT used this wireless access point to compromise track 2 data pertaining to BJ's customers. As used in this Information, "wireless access points" are devices that enable computers, including those in cash registers and inventory controllers, to connect with computer networks using radio waves.

- b. In 2004, SCOTT, accompanied and assisted by J.J., gained unauthorized access to an OfficeMax wireless access point located near the intersection of 109th Street and U.S. 1, in Miami, Florida. The pair were able to locate and download customers' track 2 debit card data, including encrypted PINs, on OfficeMax's payment card transaction processing network.
- c. Contemporaneously, SCOTT and J.J. provided the data to Gonzalez, who turned to another co-conspirator to decrypt the encrypted PINs.
- d. On July 12 and 18, 2005, SCOTT compromised two wireless access points operated by TJX Companies ("TJX") at Marshalls department stores in Miami, Florida. SCOTT used these access points repeatedly to transmit computer commands to TJX's computer servers processing and storing payment card transaction data in Framingham, Massachusetts.
- e. On September 15-16, 2005 and November 18, 2005, the conspirators downloaded payment card data stored on TJX's servers in Framingham.
- f. Beginning on May 14-15, 2006, SCOTT installed and configured a VPN connection from a TJX payment card transaction processing server to a

server obtained by Gonzalez. As used in this Information, a VPN, or “virtual private network,” is a private or secure network connection within a public computer network, such as the Internet.

- g. Beginning on May 15, 2006, and continuing for some days thereafter, including May 16, 18 and 20, SCOTT and his co-conspirators uploaded sniffer programs to a TJX payment card transaction processing server.
- h. One of the sniffer programs uploaded by SCOTT and Gonzalez was used to monitor and capture track 2 data as transactions were being processed by TJX’s network. The track 2 data captured by the sniffer program was downloaded over the VPN on numerous dates, including October 27 and December 18, 2006.
- i. In the middle of October, 2007, Gonzalez brought SCOTT to his condominium where they used a wireless access point of a nearby retailer as the vehicle for obtaining access to payment card transaction data.

All in violation of Title 18, United States Code, Section 371.

COUNT TWO
(Access Device Fraud)
18 U.S.C. § 1029(a)(3)

4. On or about September 15-16, 2005, in the Southern District of Florida, the District of Massachusetts and elsewhere,

CHRISTOPHER SCOTT

knowingly, and with intent to defraud, possessed at least 15 unauthorized access devices, to wit: credit and debit card numbers stolen from TJX.

All in violation of Title 18, United States Code, Sections 1029(a)(3) and 2.

COUNT THREE
(Aggravated Identity Theft)
18 U.S.C. § 1028A(a)(1)

5. On or about December 18, 2006, in the Southern District of Florida, the District of Massachusetts, and elsewhere,

CHRISTOPHER SCOTT

knowingly transferred, possessed, and used, without lawful authority, means of identification of others persons – to wit: credit and debit card numbers of individuals stolen from TJX – during and in relation to the commission of wire fraud (in violation of 18 U.S.C. § 1343).

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT FOUR
(Unauthorized Access to Computer Systems)
18 U.S.C. § 1030(a)(2)(C)

6. On or about November 18, 2005, in the Southern District of Florida, the District of Massachusetts and elsewhere,

CHRISTOPHER SCOTT,

by means of an interstate and foreign communication, intentionally accessed without authorization a computer, which was used in interstate and foreign commerce, and thereby obtained and aided and abetted the obtaining of information from that computer, which offense was committed for purposes of commercial advantage and private financial gain, to wit: profiting from selling stolen credit and debit card account numbers stored on computer servers operated by TJX.

All in violation of Title 18 United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i), and 2.

FORFEITURE ALLEGATIONS

18 U.S.C. § 1029(c)(1)(C)

18 U.S.C. § 982(a)(2)(B)

18 U.S.C. § 981(a)(1)(C)

28 U.S.C. § 2461(c)

7. Upon conviction of one or more offenses in violation of 18 U.S.C. § 1029, charged in Count Two of this Information, and/or § 1030, charged in Count Four herein,

CHRISTOPHER SCOTT,

defendant herein, shall forfeit to the United States: (1) any property constituting, or derived from, proceeds obtained directly or indirectly, as the result of one or more of the offenses, pursuant to 18 U.S.C. § 982(a)(2)(B); and (2) any property, real or personal, which constitutes or is derived from proceeds traceable to one or more of the offenses, pursuant to 18 U.S.C. § 981(a)(1)(C) and 20 U.S.C. § 2461(c). Such property includes, but is not limited to:

- a. approximately \$400,000 in United States currency;
- b. one men's Rolex Oyster Perpetual watch, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- c. one men's silver with clear stone ring, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- d. one men's clear stone earring, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- e. approximately \$6,000 in United States currency, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- f. one Gateway personal computer, Serial No. CSG73-A10-00215, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- g. one generic personal computer without a serial number, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- h. one Sony Vaio Laptop Computer, Serial No. 2-629-459-01, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;

- i. one 400 GB hard drive, Serial No. WMAMY1482348, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- j. one Compaq personal computer, Serial No. 6117JQHZA039, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- k. one HP Pavillion personal computer, Serial No. 2105464307254, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- l. one Toshiba Satellite personal computer, Serial No. 754424401K, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- m. one Samsung Tablet personal computer, Serial No. 409J93BLB00021E, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- n. one Sony Vaio laptop computer, Serial No. J001JETF, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- o. one Canon Rebel XT digital camera, Serial No. 1320724531, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- p. one Toshiba Satellite laptop computer, Serial No. 44325749K, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- q. one Compaq IPAQ PDA, Serial No. 4G33KVL150BV, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- r. one HP IPAQ PDA, Serial No. KRD35003GP, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- s. one 8 GB iPod, Serial No. JQ548QLDTXK, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- t. one Sony video camera, Serial No. 342124, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- u. one iPhone, Serial No. 7U728Q3TWH8, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- v. one 30 GB iPod Touch, Serial No. 9C811Z1N14N, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- w. one 2 GB iPod, Serial No. 5U549GKXSZB, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;

- x. one Sony PSP, Serial No. PP120972706-PSP1001, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- y. one Sony PSP, Serial No. PP121999429-PSP1001, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- z. one Samsung plasma, Serial No. 3910-39103CFY500218H, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- aa. one Sony Bravia plasma, Serial No. 8043089, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- bb. one Apple HD display, Serial No. CY7411C7XMP, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- cc. one Sony Bravia projector, Serial No. 2100476, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- dd. one Panoview screen, Serial No. 07011200809, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- ee. one Proview monitor, Serial No. FQQU74202277U, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008;
- ff. one Barracuda 320 GB hard drive, Serial No. 5QF052KX, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008; and
- gg. one XBOX, Serial No. 304429624705, seized from 9611 SW 148th Place, Miami, Florida on May 7, 2008.

(collectively, the "Assets").

8. Upon conviction of one of more offenses in violation of 18 U.S.C. § 1029, charged in Count Two herein,

CHRISTOPHER SCOTT,

defendant herein, shall forfeit to the United States any personal property used or intended to be used to commit the offense, pursuant to 18 U.S.C. § 1029(c)(1)(C). Such property includes, without limitation, the Assets.

9. If any of the property described in paragraphs 7 and 8, as a result of any act or

omission by the defendant –

- a. cannot be located upon the exercise of due diligence,
- b. has been transferred or sold to, or deposited with, a third party,
- c. has been placed beyond the jurisdiction of the Court,
- d. has been substantially diminished in value, or
- e. has been commingled with other property which cannot be subdivided without difficulty,

it is the intention of the United States, pursuant to 18 U.S.C. § 1029(c)(2) and/or § 982(b)(1), both of which incorporate 21 U.S.C. § 853(p), to seek forfeiture of any other property of the defendant up to the value of the property described above.

All pursuant to Title 18, United States Code, Sections 981, 982 and 1029, and Title 28, United States Code, Section 2461.

MICHAEL J. SULLIVAN
United States Attorney

By:


STEPHEN P. HEYMANN
Assistant U.S. Attorney

DATE: August 5, 2008